REMARKS

In response to the Final Office Action mailed April 16, 2007, Applicants respectfully request entry of this amendment. Claims 7-31 were previously pending in this application. Claims 7, 14, 15, 17-19, 21, 23, 24 and 31 have been amended. As a result, claims 7-31 are pending for examination with claims 7, 19, and 24 being independent. No new matter has been added.

Rejections under 35 U.S.C. §112

The Office Action rejected claims 7-31 under 35 U.S.C. 112, second paragraph, as being indefinite. Applicants have amended claims 7, 19, and 24 to address the concerns noted in the Office Action.

Accordingly, withdrawal of this rejection is respectfully requested.

Rejections Under 35 U.S.C. §102

The Office Action rejected claims 7-31 were rejected under 35 U.S.C. 102(e) as being anticipated by Terzis et al., US Published Patent Application No. 20040243835 (Terzis). Applicants respectfully disagree. Applicants respectfully traverse the rejection of claims 7-31 for the reasons discussed below.

First, claim 7, as amended, recites:

> An object model embodied on a computer-readable medium for managing a service on a computer, the object model comprising:
>
> a policy object model for specifying, *by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user*; and
>
> a policy engine platform for interacting of the first user with the at least one first policy and of the second user with the at least one second policy, and to provide the at least one first policy and the at least one second policy to at least one component that performs the service.
>
> (Emphasis added).

Terzis is directed to a computer-based system for providing secure, configurable access to computer network resources (Abstract). A human-readable language for defining access policy rules is provided, with these rules converted in an automated fashion into filters applied within the various subsystems and components in the multiplayer security system (page 2, ¶ 0018). The rules may be generated and installed at different levels (page 2, ¶ 0020). A system administrator uses user interfaces to create access/security rules that allow users access to specific network resources based on a variety of parameters including group membership and time of day (page 4, ¶ 0056). The administrator 310 configures the MACSS 300 by providing user information 312, group information 314, and access rules 316 (page 4, ¶ 0058, FIG. 3). The administrator may resolve conflicts which arise when a new rule is added to the policy database 820 and validation tests performed to ensure that the new rule does not conflict with existing policy rules that return an error message (page 6, ¶ 0079, FIG. 8).

Terzis neither discloses nor suggests that a policy may be specified by a first user or by a second user. In contrast, claim 1 recites specifying, by *a first user,* if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, *at least one first policy that the service supports in a packet-centric form*, and, *by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user*. (Emphasis added).

The Office Action states that Terzis teaches determining whether a requester is authorized, which comprises comparing a provider rank for the requester against a permitted rank. However, Terzis describes that the permission level can have different values depending on whether the resource described in the rule is an L4 resource or a URL resource (page 9, ¶ 0121). In the case of L4 resources, the permission level can be accept, drop (no response back to requester), or deny (negative response is sent back to the requestor). In the case of URL resources, the permission level can be read, write, or execute (page 9, ¶ 0121). In contrast, as described on page 25, ¶ 0051 of the specification of the present application, policy providers may be ranked in accordance with their individual priorities. Therefore, Terzis neither discloses nor suggests "specifying, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy," as recited in claim 1.

Therefore, Terzis neither discloses nor suggests "an object model embodied on a computer-readable medium for managing a service on a computer, the object model comprising: a policy object model for specifying, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user; and a policy engine platform for interacting of the first user with the at least one first policy and of the second user with the at least one second policy, and to provide the at least one first policy and the at least one second policy to at least one component that performs the service," as recited in claim 7.

In view of the foregoing, claim 7 patentably distinguishes over Terzis.

Claims 8-18 depend from claim 7 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 7-18 is respectfully requested.

<u>Second</u>, claim 19, as amended, recites:

> A method of managing a service on a computer, the method comprising:
>
> *specifying, via a policy object model, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified use*r;
>
> interacting, via a policy engine platform, of the first user with the at least one first policy, and of the second user with the at least one second policy; and
>
> providing, via the policy engine platform, the at least one first policy and the at least one second policy to at least one component that performs the service.
>
> (Emphasis added).

As discussed above, Terzis neither discloses nor suggests "a method of managing a service on a computer, the method comprising: specifying, via a policy object model, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the service supports in a packet-centric form, and, by a second, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user;

interacting, via a policy engine platform, of the first user with the at least one first policy, and of the second user with the at least one second policy; and providing, via the policy engine platform, the at least one first policy and the at least one second policy to at least one component that performs the service," as recited in claim 19.

In view of the foregoing, claim 19 patentably distinguishes over Terzis.

Claims 20-23 depend from claim 19 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 19-23 is respectfully requested.

<u>Third,</u> claim 24, as amended, recites:

> An object model embodied on a computer-readable medium for managing a firewall service on a computer, the object model comprising a policy object model used to *specify, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the firewall service supports in a packet-centric form, and, by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user*, the policy model comprising a policyrule object usable to generate a policy, the policyrule object comprising a condition property and an action property, wherein the policy generated by the policyrule object is configured to perform an action specified in the action property responsive to a condition specified in the condition property being met.
>
> (Emphasis added).

Terzis neither discloses nor suggests "an object model embodied on a computer-readable medium for managing a firewall service on a computer, the object model comprising a policy object model used to specify, by a first user, if it has been determined that the first user is authorized to perform the specification by comparing a rank of the first user against a permitted rank, at least one first policy that the firewall service supports in a packet-centric form, and, by a second user, at least one second policy by selecting a security level from a plurality of security levels, with each security level from the plurality of security levels being previously set for a specified application and a specified user, the policy model comprising a policyrule object usable to generate a policy, the policyrule object comprising a condition property and an action property, wherein the policy generated by the policyrule object is configured to perform an action specified in the action property responsive to a condition specified in the condition property being met," as recited in claim 24.

In view of the foregoing, claim 24 patentably distinguishes over Terzis.

Claims 25-31 depend from claim 24 and are allowable for at least the same reasons.

Therefore withdrawal of the rejection of claims 24-31 is respectfully requested.

CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: June 15, 2007

Respectfully submitted,

By: ______________________
James H. Morris, Reg. No. 34,681
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
Telephone: (617) 646-8000